(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 217 497 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.06.2002 Bulletin 2002/26

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **01310428.6**

(22) Date of filing: **13.12.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **20.12.2000 JP 2000387833**

(71) Applicant: **Sega Corporation**
Ohta-ku, Tokyo 144-8531 (JP)

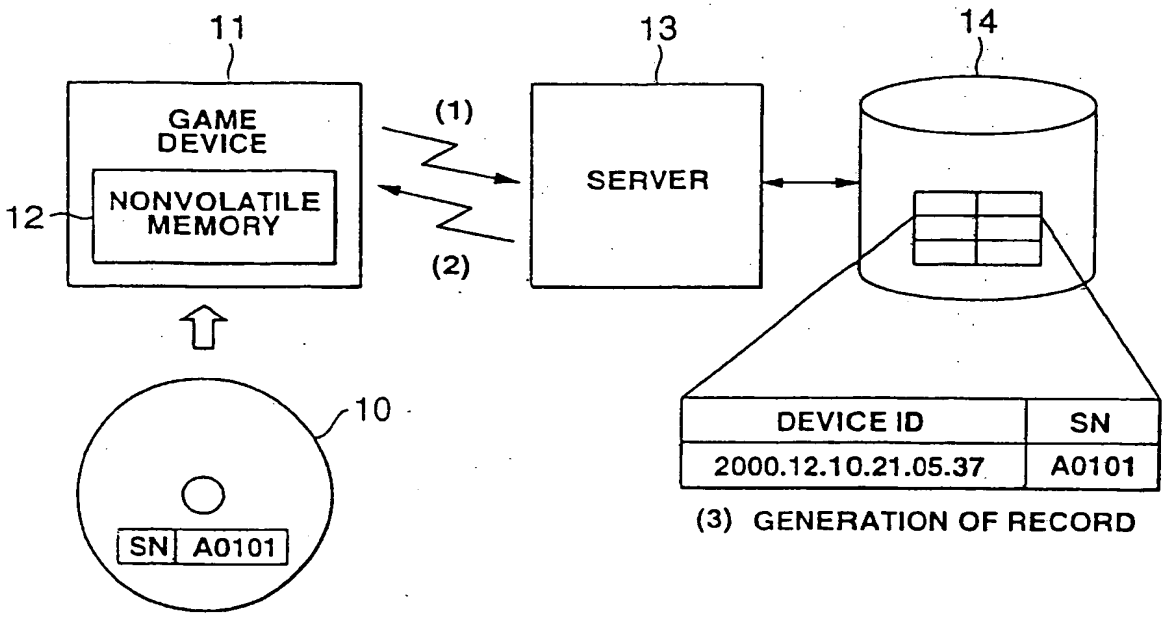
(72) Inventors:
- **Miyoshi, Takao**
  Ohta-ku, Tokyo 144-0043 (JP)
- **Setsumasa, Akio**
  Ohta-ku, Tokyo 144-0043 (JP)

(74) Representative: **Brown, Kenneth Richard**
R.G.C. Jenkins & Co.
26 Caxton Street
London SW1H 0RJ (GB)

(54) Security system for game devices connected with a server

(57) Provided is a security system for managing which CD-ROM is used for a game device not having identifying information in advance. When a game device accesses a server via a communication network, a device ID, which is issued from the server, is stored in a nonvolatile memory. This device ID is generated based on the time and date when the game device accesses the server via a communication network (e.g. December 10, 2000 at 21:05:37). The server associates a serial number (SN) of a CD-ROM used in the game device and a device ID of the game device with each other and registers them on a database .This makes it possible to manage which CD-ROM is used in each game device .

FIG.1



EP 1 217 497 A2

Description

BACKGROUND OF THE INVENTHION

1. Field of the Invention

[0001] The present invention relates to technology for security system, more particularly to a communication game system by connecting a plurality of game devices through a network.

2. Description of the Related Art

[0002] It has been suggested that a communication game system is realized by connecting a plurality of game devices to a communication network such as a telephone line, an ISDN network, etc. In such communication game system, the applicant suggested a security technology of a recording medium in Japanese Patent Laid-Open Publication No. 2000-35885 in order to prevent a third party from misusing a recording medium with game software stored therein.

[0003] The Publication describes the technology in which a server manages identifying information inherent in a recording medium with game software stored therein and identifying information inherent in a game device to understand which recording medium is used in each game device, whereby, when such game device is connected to a communication network, a limitation is imposed on game processing if such server judges that the recording medium attached to the game device was previously used in another game device, and ordinary game processing is performed if the server judges that such recording medium is being used only for the pertinent game device.

[0004] However, as identifying information inherent in a game device is not always pre-recorded in the phase of developing such game device, there is also a game device not having such identifying information.

[0005] Further, in communication games, a game play could be resumed from the status immediately before stopping play of the game last time by backing up data, such as the progression status of the game or various items which a player obtained, in a backup memory which is detachable from a game device body or an operation controller. However, as one's own data (e.g. items, etc.) could be provided to a third party by copying the contents of the backup memory, such third party could enjoy playing the game using another person's saved data. Thus, when the contents of a backup memory can easily be copied, the problem will arise that a player can not fully enjoy the game.

[0006] Such problem will also arise when a backup memory detachable from a game device body or an operation controller is attached to another person's game device or operation controller to play a game.

[0007] Furthermore, saved data which is backed up in a backup memory can be transferred from a game device to another game device through a communication network; however, if the saved data, upon transferring the saved data from the backup memory to the game device, remained in the backup memory, there is the possibility of misuse by providing saved data to another person while retaining the saved data in one's own backup memory by forcibly taking the backup memory from the game device.

[0008] Also, in conventional communication games, there was no limitation of the levels required to participate in a game. Accordingly, for example, when a beginner and a skilled player participate in a communication game, the beginner will reach the ending of the game by doing nothing but following the skilled player, which reduces the amusing aspect of the game.

[0009] Similarly, when, in a communication game in which a plurality of players participates, saved data concerning progression status of the game is backed up, a beginner will start the game in the middle of a skilled player's game by participating in the game with the skilled player. If the saved data concerning the progression status of the game is backed up in a beginner's backup memory, the next game will start in the middle of such game and a part of the game will become unable to be played, it, therefore, is not desirable.

[0010] Further, as long as a communication game is connected to a telephone line, the telephone bill is charged as a connection fee, and in addition, a fee for an Internet connection to the provider is also charged. Therefore, when it unnecessarily takes a long time at the ending part of the game, which does not require the operation by a player, the player is forced to be responsible for costly charges.

[0011] Here, an object of the present invention is to provide a computer readable recording medium in which a security system for preventing misuse by a third party of a recording medium, a data processing device, a recording medium management method and a program for performing such method are recorded. Another object of the present invention is to provide a computer readable recording medium in which a data processing device for preventing misuse of a backup memory, a data processing method, a security system, a method for managing saved data and a program for performing such method are recorded. Still another object of the present invention is to provide a computer readable recording medium in which a game server for enhancing an amusing aspect of a communication game, a game processing method and a program for performing such method are recorded.

SUMMARY OF THE INVENTION

[0012] To solve the aforementioned problems, in the present invention, identifying information inherent in a data processing device connected to a communication network is issued, the identifying information inherent in the data processing device and identifying information

inherent in a recording medium in which data to be processed in the data processing device is recorded are associated with each other and stored, and in reference to such association, which data processing device is used in each recording medium is managed. As identifying information of a data processing device is issued by a server via a communication network, even though the data processing device does not have inherent identifying information in advance, security of the recording medium can be secured.

[0013] Further, the present invention can provide a computer readable recording medium in which a program for causing a computer system to perform the aforementioned method is recorded. Examples of computer readable recording media are: in addition to portable recording media such as optical disks (disks having an inherent physical format such as CD-ROM, DVD-ROM, DVD-RAM, DVD-R, PD Disk, MD Disk, MO Disk, etc.) and flexible disks, internal recording devices in a computer such as RAM or ROM, etc., or external recording devices such as a hard disk.

[0014] Furthermore, in the present invention, saved data in a backup memory is encrypted using identifying information inherent in the data processing device as a key. By this, the saved data in the backup memory can not be used in another data processing device, and therefore, misuse of the saved data can be prevented.

[0015] In the present invention, also, after saved data to be processed in a data processing device is transferred to a data processing device, the saved data stored in a nonvolatile memory within a backup memory is deleted, which effectively prevents misuse of transferring saved data in a backup memory to another data processing device while retaining such data in the backup memory.

[0016] In the present invention, also, the number of times which a data processing device having a backup memory is connected to a communication network is registered in a database while such number of times is recorded in the backup memory or data processing device, and when such number of times, which is obtained from the data processing device upon the data processing device having a backup memory being connected to the communication network, is consistent with the number of times registered in the database, the processing of data in the backup memory is permitted. By this, illegitimate copy of the data in the backup memory can be effectively prevented.

[0017] In the present invention also, a level required to participate in a game is set in advance in accordance with the difficulty of the game and a player complying with the required level for the difficulty of the game is allowed to participate in the game. This can solve the aforementioned problem that a beginner proceeds through a communication game with help from a skilled player by participating in the game with the skilled player.

[0018] Further, in the present invention, progression status of a communication game is not backed up as saved data when such game is played via a communication network. Even in the case in which a game device backs up progression status of the game, it may be prohibited to start a game in the middle of the game in reference to such progression status when the game is played without connecting to a communication network. This can solve the aforementioned problem.

[0019] Furthermore, in the present invention, the displaying time of an ending screen of a communication game, when such game is played via a communication network, is shortened. This can reduce an increase in a fee for a connection to a communication network and a fee for an Internet connection to a game server.

BRIEF DESCRIPTION OF THE DRAWTNGS

[0020] Figure 1 is an illustration of a security system of a recording medium.

[0021] Figure 2 is an illustration of a game device and a controller.

[0022] Figure 3 is an illustration of an exterior view of a game device and a controller.

[0023] Figure 4 is an illustration showing a structure of a connection between game devices and a communication network.

[0024] Figure 5 is an illustration showing a transfer of saved data.

[0025] Figure 6 is an illustration of a security system for a backup memory.

[0026] Figure 7 is an illustration of prevention of an illegitimate copy of a backup memory.

[0027] Figure 8 is an illustration of a communication game.

[0028] Figure 9 is an illustration of levels required to participate in a communication game.

[0029] Figure 10 is an illustration of a plot of a game development.

[0030] Figure 11 is a flowchart relating to backing-up of flag data showing progression status of a game.

[0031] Figure 12A,12B,12C,12D and 12E is an illustration of ending screens of a game.

DESCRIPTION OF THE PREFFERD EMBODIMENT

Embodiment 1

[0032] Figure 1 is an illustration of a server, which prevents misuse by a third party of a recording medium, and a game device. In the Figure, numeral 10 is a portable recording medium such as a CD-ROM with game software stored therein, and numeral 11 is a home game device. The game device 11 comprises desired communication functions so as to read a game program recorded in the recording medium 10 and play a communication game together with another game device through a communication network such as a public circuit (e.g. telephone line, ISDN network, etc.) or an exclusive circuit.

A server 13 manages the communication game processing, etc. of each game device connected to the communication network.

[0033] In the recording medium 10, identifying information inherent in each recording medium, which is called a "serial number (SN)" is provided. In the example of Figure 1, the SN of the recording medium is A0101. The SN may be the one recorded in the recording medium 10 as data or the one indicated in its package or manual. When the game device 11 accesses the server 13 through a communication network (Figure 1 (1)), the server 13 requires the game device 11 to transfer the device ID of the game device 11 and the SN of the recording medium 10. The device ID is identifying information allocated to each game device so it does not overlap with others and is issued from the server 13.

[0034] When the game device 11 first accesses the server 13, the server 13 issues a device ID to the game device 11 as it did not yet issue the device ID to the game device 11 (Figure 2 (2)). As a device ID, the time of the game device 11 accessing the server can be used. The time includes the year, month, day, hour, minute and second. When the time and the date of access is December 10, 2000 and 21:05:37, for example, the device ID is 2000.12.10.21.05.37. The game device 11 stores the device ID issued from the server 13 on a nonvolatile memory 12 such as a flash memory. Further, the data encrypted by time and date may be stored in the nonvolatile memory 12 as a device ID.

[0035] In a database 14, the SN of a recording medium used in the game device using the device ID as a key is associated and managed in each record. The server 13 generates a record in which the device ID issued to the game device 11 (2000.12.10.21.05.37) and the SN (A0101) are associated with each other (Figure 1 (3)).

[0036] By the aforementioned structure, the server 13 associates the device ID of the game device 11 and the SN of the recording medium 10 with each other and manages them. Therefore, if a third party attempts to insert a recording medium used in another game device into its own game device and use it, the SN of the recording medium and the device ID of the game device are not consistent with each other, and therefore, the server 13 can impose a limitation on the use by such third party of the recording medium.

[0037] Further, considering that there is almost no possibility that no less than two players simultaneously access the server, including the same second, upon using as a device ID the time and date (at the same second) for accessing the server 13, a device ID inherent in each game device can be practically allocated to each game device. Of course not only can the time and date of the game device accessing the server be used as a device ID, but also an ID provided in advance to avoid an overlap can be used as a device ID.

[0038] Furthermore, in the above explanation, although a CD-ROM is referred to as an example of a recording medium, it does not limit it, as optical disks (e. g. DVD-ROM, DVD-RAM, DVD-R, PD Disk, MD Disk, MO disk, etc.), a flexible disk (FD), a detachable cartridge in which a game program is stored, a memory card, etc. can also be used.

Embodiment 2

[0039] Figure 3 is an illustration of a game device and an operation controller. In an operation controller 20, a backup memory 22 for saving saved data is detachable and an operating unit 21, on which an analog key or switches are arranged, is provided. The backup memory 22 includes a nonvolatile memory. The operation controller 20 is connected to a game device 23 via a connection cord 28 and a connector 29. Further, the backup memory 22 may be attached to the game device so as to be directly and freely detachable therefrom.

[0040] Figure 2 is a functional block diagram of a game device and an operation controller. A game device 23 comprises a game processing unit 24, an encrypting unit 25, a CD-ROM drive 26 and a device ID memory 27. These modules are realized by hardware, such as a CPU, a ROM, a RAM, etc. In the game processing unit 24, a game program to be supplied from a CD-ROM via the CD-ROM drive 26 is read and a game program is executed based on a control signal of the analog key or switches which is outputted from the operating unit 21, and saved data to be backed up in the backup memory 22 is generated.

[0041] When a player directs the game device 23 to back up saved data in the backup memory 22, or directs the game device 23 for a game program to back up saved data in the course of program processing, the encrypting unit 25 encrypts the saved data using, as a key, information inherent in the game device 23 stored in the device ID memory 27 (e.g. production number), and backs up such data in the backup memory 22. For encryption, a known encryption technology can be used. Meanwhile, when the game device 23 reads the saved data backed up in the backup memory 22, the saved data is decrypted in the encrypting unit 25 using the device ID as a key, and is outputted into the game processing unit 24.

[0042] By the above structure, the data saved in the backup memory 22 is encrypted using the information inherent in the game device 23 as a key, and therefore, such data can not be used in another game device. Accordingly, misuse of a backup memory, such as playing a game in one's own game device using another's backup memory, can be effectively prevented.

Embodiment 3

[0043] Figure 4 is an illustration of the case in which a plurality of game devices is connected to a communication network to play a game. In the Figure, numerals 32 and 34 are home game devices, and numeral 35 is

a server for controlling a communication game. Numeral 36 is a communication network such as a public circuit. An operation controller 31, which comprises a backup memory 310 for backing up saved data, is connected to the game device 32. Likewise, an operation controller 33, which comprises a backup memory 330, is also connected to a game device 34. For a communication protocol in the communication network 36, TCP/IP, which is suitable for an open network, is used.

[0044] The game device 32 timely writes in a ROM 320 an item obtained by a player, the score, progression status of a game, etc. along with the progression of the game. The data written in the RAM 320 can be transferred to the backup memory 310 as saved data. Further, the items, etc. obtained by the player can be transferred to a RAM 340 of the game device 34 via the communication network 36.

[0045] Figure 5 is an illustration showing status of a backup memory when a communication game is played using saved data backed up in the backup memory. In the backup memory 310, saved data such as items is backed up. When the game device 23 is connected to a network, the saved data in the backup memory 310 is transferred (moved) to the RAM 320 of the game device 23, and the saved data in the backup memory 310 is deleted. Thus, while the game device 23 is connected to the communication network 36, the saved data in the backup memory 310 is vacant. At the time of ending the game, when the saved data in the RAM 320 is backed up in the backup memory 310, the saved data is transferred from the RAM 320 to the backup memory 310.

[0046] Conventionally, when the saved data in the backup memory 310 is transferred to the RAM 320, the saved data is copied to be transferred; therefore, the saved data is also backed up in the backup memory 310 even after the saved data is transferred to the RAM 320. As a result, even in the case that a player provides another player with a part of or the whole parameters in the saved data, by forcibly taking the backup memory 310 from the operation controller 31 thereafter, the saved data provided to such other player can be backed up in the player's own backup memory 310.

[0047] According to this embodiment, however, the saved data in the backup memory 310 is not copied to the RAM 320, but transferred to the RAM 320, which can effectively prevent misuse of the backup memory as described above.

Embodiment 4

[0048] Figure 6 is an illustration of a server, which controls a communication game and a game device. In the Figure, numeral 41 is a home game device, by which a game can be played by accessing a server 44. The game device 41 develops a game based on an operation signal supplied from an operation controller 42. The controller 42 comprises a backup memory 43 for backing up saved data. The backup memory 43 comprises a nonvolatile memory.

[0049] The server 44 comprises a database 45 and records by record the number of access times and the time and date of access (hereinafter referred to as the "Access Information") using its device ID as a key. The device ID is information inherent in the game device 41, e.g. the production number, the time (including the second) and date when the game device 41 is first connected to a network, etc. In the example of Figure 6, the device ID of the game device 41 is B1011, the number of access times is 72, the time and date of access is October 2, 2000, 19:14:32, October 4, 2000, 21:25:11, October 9, 2000, 11:07:52. While the Access Information of the game device 41 is registered in the database 45, the same content of such information is also written in the backup memory 43.

[0050] In Figure 6, when the game device 41 accesses the server 44 via a communication network (Figure 6 (1)), the server 44 obtains from the game device 41 the device ID and the Access Information in the backup memory 43. Then, in reference to the database 45 (Figure 6(2)), the consistency of the device ID and the Access Information is checked. Considering that there is almost no possibility that a plurality of game devices access the server at the same time and date including the same second, the Access Information can be considered inherent in the backup memory 43. Therefore, the Access Information of the game device functions as identifying information for distinguishing the backup memory 43 from another backup memory.

[0051] When the device ID and the Access Information are consistent with each other, the server 44 increments the number of access times by one and updates the records by adding and recording such time and date of access. Simultaneously, the information of the backup memory 43 is also updated (Figure 6(3)). Meanwhile, when the device ID and the Access Information are not consistent with each other, there is a doubt raised of misuse of the backup memory 43, and therefore, the use of the backup memory is restricted.

[0052] The inconsistency of the device ID and the Access Information refers to ① the case of attempting to back up saved data in another person's backup memory and to use such data, and ② the case of there being a doubt raised of illegitimately copying the saved data. In the case of ①, the device ID and the number of access times, and the time and date of access are completely inconsistent with each other. Therefore, it is obviously an attempt to use another's saved data not used in the game device 41. In the case of ②, the saved data is the one used in the game device 41, the access time and date is partly consistent, but there is a doubt raised of illegitimate copying because of the inconsistency of the number of access times.

[0053] The case of ② is explained in detail in reference to Figure 7. As shown in the Figure, the saved data backed up in the backup memory 43 is illegitimately copied in a backup memory 46 (Figure 7 (1)). If the number

of access times recorded in the backup memory 43 is 72, the number of access times recorded in the backup memory 46 also becomes 72. Here, when a player uses the backup memory 43, such number of access times recorded in the backup memory 43 is updated to be 73 (Figure 7(2)). Further, the record in the database 45 is also updated to be 73 (Figure 7 (3)). Here, when the player takes the backup memory 43 from the controller 42 and newly attaches the backup memory 46 and accesses the server 44, it becomes clear that there is a doubt raised of illegitimate copying as the number of access times in the backup memory 46 and that recorded in the database 45 are different (Figure 7 (4)). Further, the same is the case of using the same backup memory, such as the case of copying in advance saved data in another recording medium, then playing a game, and updating saved data and setting such saved data back again to the one before such update and then playing a game.

[0054] As described above, according to this embodiment, the server 44 manages the device ID and the Access Information of the game device 41, and therefore, misuse of the backup memory 43 and an illegitimate copy can be effectively prevented by cross-checking the device ID and the Access Information.

Embodiment 5

[0055] Figure 8 is an illustration of the case of playing a communication game by connecting a plurality of game devices to a communication network. In the Figure, numerals 51 to 53 are game devices connected to a communication network 54 and numeral 55 is a server for controlling a communication game. In this embodiment, as shown in Figure 9, a level required to participate in a communication game is set in accordance with the level of the game. For instance, at the basic level, everyone can participate in the game; however, at the advanced level, a level of no less than 20 is required to participate in the game, and at the expert level, a level of no less than 40 is required to participate in the game. The "level" referred to here means a parameter to be given to a player' s character as the game proceeds, which is mainly given in accordance with the kind and number of enemy characters which the player's character defeated during the game.

[0056] Figure 8 shows the level of each player in the case of playing a communication game of high level. The level of a player for a game device 51 is 25, that for a game device 52 is 30 and that for a game device 53 is 45; therefore, the communication game of high level can be played by these three players.

[0057] Conventionally, when such communication game is played by a plurality of players, a player can participate in the game regardless of his/her level. Therefore, for instance, a skilled player who is familiar with communication games and a beginner who has just started to play communication games can play a game together, and the beginner would be able to reach the ending of the game by following the skilled player. If voluntary participation in a communication game regardless of the levels is allowed, the amusing aspect of the game may be reduced. According to this embodiment, however, the level of a player who is allowed to participate in a communication game is set in accordance with the level of the game, which can solve the aforementioned problem.

[0058] Figure 10 is an illustration showing a plot of a game development. As shown in the Figure, the game consists of stages 1 to 3. The stages consist of the scenes such as a forest area, an underground cave, a dig and an ancient space ship. In each such stage, a scene 1 and a scene 2 are set in line with the proceeding of the game, which provides variation to the development of the scenes. Each stage has a final scene and a player can proceed to the next stage by defeating an enemy character appearing in the scene.

[0059] When a player plays a game off line without connecting to a communication network, generally, progression status of the game is backed up as flag data in preparation for the next game play. However, upon playing a game on line via a communication network, a plurality of players' characters develop the game, and therefore, for instance, even though a beginner does nothing, such beginner can proceed through the game only by following a high-level player.

[0060] As a result, in this embodiment, as shown in Figure 11, upon playing a game on line (Step S1; YES), flag data showing progression status of the game is not backed up (Step S2), and upon not playing a game on line (Step S1; NO), flag data showing progression status of the game is backed up (Step S3). By such structure, the aforementioned problem can be solved. Further, even if the case in which the game device stores flag data showing progression status of the game, it may be prohibited for a player to play a game in the middle thereof in reference to the flag data when the game is played without connecting to a communication network.

[0061] Further, as means for controlling the back-up of flag data showing progression status of a communication game, back-up controlling means may be provided for the game device, and the back-up of flag data showing the progression status of the game may be controlled by the game server.

Embodiment 7

[0062] Figure 12 shows changes of ending screens of a game. In the Figure, Figures 12A to 12C are diagrams of changes of ending screens when a player plays a game off without connecting to a communication network, and then ends the game. When a player character 61 defeats an enemy character 62 and ends the game (figure 12A), the credits are run for several minutes (figure 12B), and the "END" screen is displayed (figure 12C).

[0063] Meanwhile, Figures 12D and 12E are diagrams of changes of ending screens when a plurality of players play a game on line via a communication network and then end the game. When players' characters 71 to 74 defeat an enemy character 75 and end the game (Figure 12D) , the "END" screen is promptly displayed (Figure 12E), and then returned to the initial screen (Figure 12D).

[0064] Thus, when a player plays a communication game on line, as long as the game is connected, a fee for an Internet connection to a server is charged in addition to a fee for a connection to a telephone line. Therefore, by shortening the time of the ending screens of the game, the player's costs can be reduced.

[0065] Furthermore, in the case of a communication game, as means for controlling the shortening of the displaying time of the ending screens of the game, such controlling means may be provided for the game device, the displaying time of the ending screens may be shortened by a game server.

[0066] According to the present invention, identifying information is issued from a server to a data processing device via a communication network. Therefore, even if no identifying information is provided to a data processing device in advance, it is possible to manage which recording medium is used in which data processing device.

[0067] According to the present invention, saved data in a backup memory can be encrypted and decrypted using, as a key, identifying information inherent in a data processing device, which is effective for protecting the security of the saved data.

[0068] According to the present invention, saved data backed up in a nonvolatile memory of a backup memory is deleted after the saved data to be processed to a data processing is transferred to the data processing device, which can effectively prevent misuse of saved data.

[0069] According to the present invention, a server manages the number of times that a data processing device having a backup memory is connected to a communication network, which can effectively prevent misuse of the saved data in the backup memory.

[0070] According to the present invention, a level required to participate in a communication game is set in advance in accordance with the difficulty of the game, a player complying with the level required in accordance with the difficulty of the game is allowed to participate in the communication game, which enables the communication game to be more amusing.

[0071] According to the present invention, progression status of a game is not backed up as saved data when the game is played via a communication network, which enables the communication game to be more amusing.

[0072] According to the present invention, the displaying time of ending screens of a communication game is shortened when the game is played via a communication network, which can reduce the burden of a connection fee to a communication network.

[0073] The invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. The present embodiment is therefore to be considered in all respect as illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than by the forgoing description and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

Claims

1. A security system comprising:

   means for issuing identifying information inherent in a data processing device connected to a communication network;
   means for associating said identifying information inherent in said data processing device and identifying information inherent in a recording medium in which data to be processed in said data processing device is recorded with each other and storing them; and
   means for, in reference to said association, managing which recording medium is used in each said data processing device.

2. A security system according to claim 1, wherein the time of said data processing device being connected to a communication network or information using said time is used as said identifying information inherent in said data processing device.

3. A method for managing a recording medium comprising the steps of:

   issuing identifying information inherent in a data processing device connected to a communication network;
   associating said identifying information inherent in said data processing device and identifying information inherent in a recording medium in which data to be processed in said data processing device is recorded with each other and storing them; and,
   in reference to said association, managing which recording medium is used in each said data processing device.

4. A method according to claim 3, wherein the time of said data processing device being connected to a communication network or information using said time is used as said identifying information inherent in said data processing device .

5. A computer readable recording medium with a pro-

gram stored therein for causing a computer system to perform a method according to claim 3 or 4.

6. A data processing device comprising:

storing means for storing first identifying information inherent in a data processing device which is issued from a server via a communication network; and
sending means for sending said first identifying information and second identifying information inherent in a recording medium with a data stored therein associated with said first identifying information to manage a recording medium to server via a communication network.

7. A computer readable recording medium with a program stored therein for causing a computer system to perform a method according to claim 6.

8. A data processing device for processing saved data in a backup memory, comprising :

means for storing identifying information inherent in said data processing device;
means for encrypting said saved data using said identifying information inherent in said data processing device as a key.

9. A data processing device according to claim 8, further comprising means for decrypting said encrypted saved data using said identifying information as a key.

10. A data processing method for encrypting saved data in a backup memory using identifying information inherent in a data processing device as a key.

11. A data processing method according to claim 10, which decrypts said encrypted saved data using said identifying information as a key.

12. A computer readable recording medium with a program stored therein for causing a computer system to perform a method according to claim 10 or 11.

13. A data processing device comprising:

means for reading and storing saved data from a backup memory and
means for deleting said saved data backed up in said backup memory after said reading of said saved data.

14. A method for managing a saved data comprising the steps of:

transferring saved data to be processed in a data processing device from back up memory to said data processing device, and
deleting said saved data backed up in a non-volatile memory of a backup memory thereafter.

15. A security system comprising:

means for registering in a database the number of times that a data processing device having a backup memory is connected to a communication network while recording said number of times in said backup memory or said data processing device and
means for, upon said data processing device being connected to a communication network, when said number of times obtained from said data processing device is consistent with the number of times registered in said database, permitting the processing of said data in said backup memory.

16. A security system according to claim 15, wherein the time when said data processing device having said backup memory is connected to a communication network or information using said time is used as identifying information inherent in said backup memory.

17. A method for managing a saved data comprising the steps of:

registering in a database the number of times that a data processing device having a backup memory is connected to a communication network while recording said number of times in said backup memory and said data processing device; and,
upon said data processing being connected to a communication network, when said number of times obtained from said data processing device is consistent with the number of times registered in said database, permitting the processing of the data in said backup memory.

18. A method according to claim 17, wherein the time when said data processing device having said backup memory is connected to a communication network or information using said time is used as identifying information inherent in said backup memory.

19. A computer readable recording medium with a program stored therein for causing a computer system to perform a method according to claim 17 or 18.

20. A game server comprising:

means for setting in advance a level required to participate in a communication game in accordance with the difficulty of said game; and
means for allowing a player complying with the required level according to the difficulty of said game to participate in said communication game.

21. A game processing method for not saving progression status of a game when a communication game is played via a communication network.

22. A computer readable recording medium with a program stored therein for causing a computer system to perform a method according to claim 21.

23. A game processing method for shortening a displaying time of an ending screen of a game when a communication game is played via a communication network.

24. A computer readable recording medium with a program stored therein for causing a computer system to perform a method according to claim 23.

FIG.1

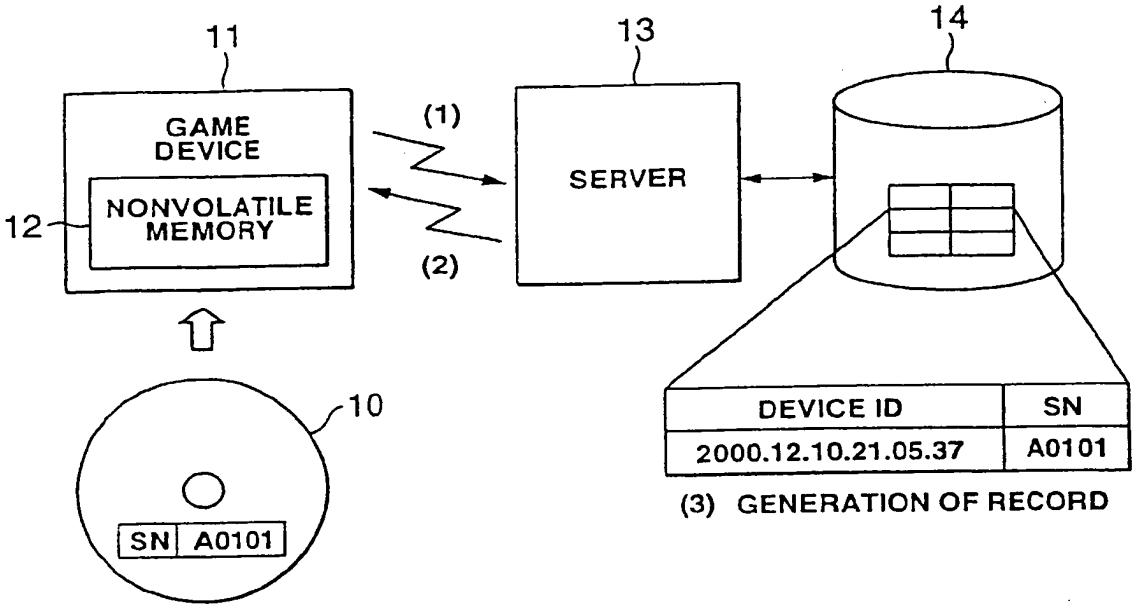

11
13
14
GAME DEVICE
NONVOLATILE MEMORY
12
(1)
(2)
SERVER
10
SN A0101
DEVICE ID
SN
2000.12.10.21.05.37
A0101
(3) GENERATION OF RECORD

FIG.2

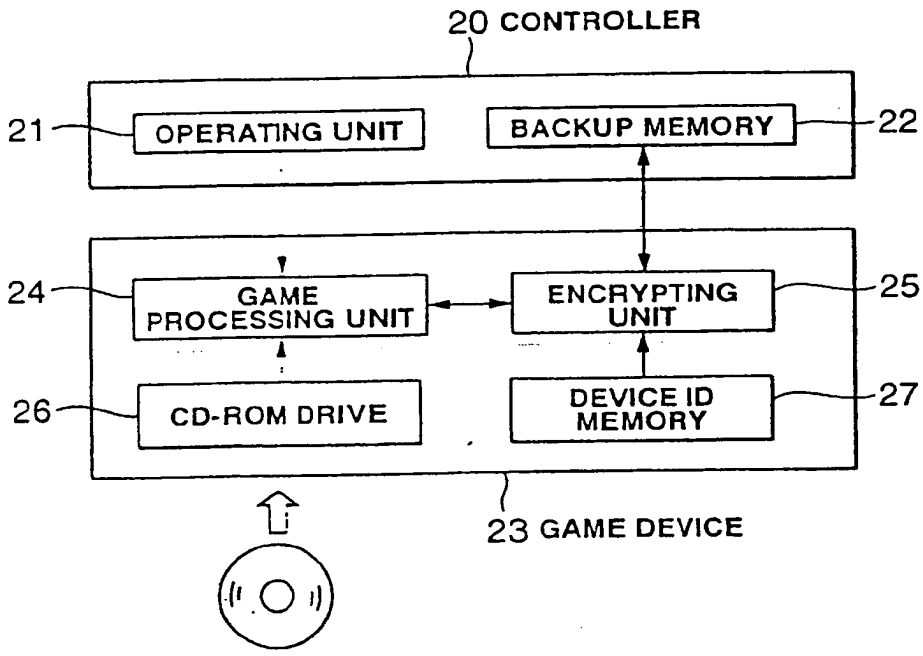

20 CONTROLLER
21
OPERATING UNIT
BACKUP MEMORY
22
24
GAME PROCESSING UNIT
ENCRYPTING UNIT
25
26
CD-ROM DRIVE
DEVICE ID MEMORY
27
23 GAME DEVICE

FIG.3

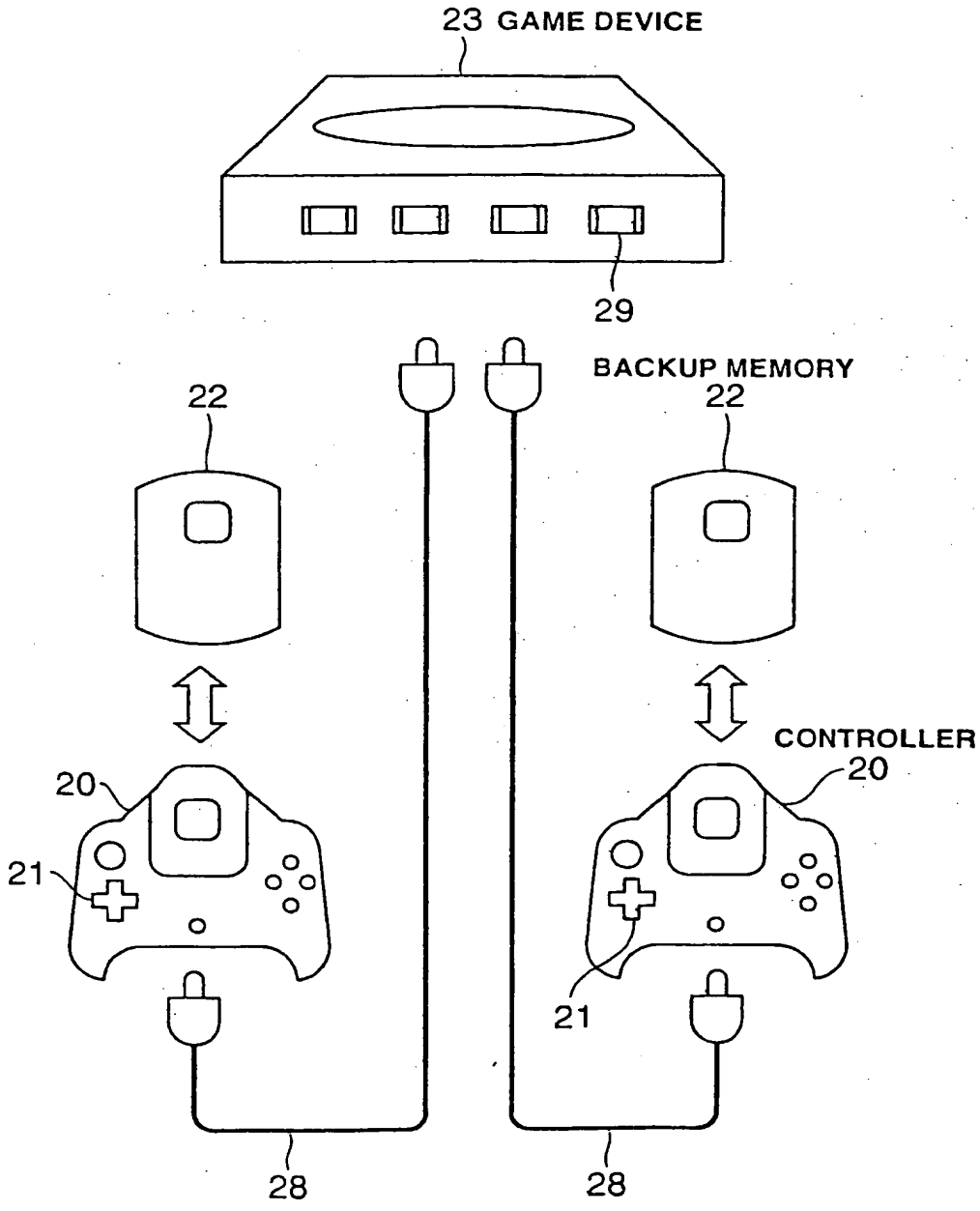

23 GAME DEVICE
29
BACKUP MEMORY
22
22
CONTROLLER
20
20
21
21
28
28

FIG.4

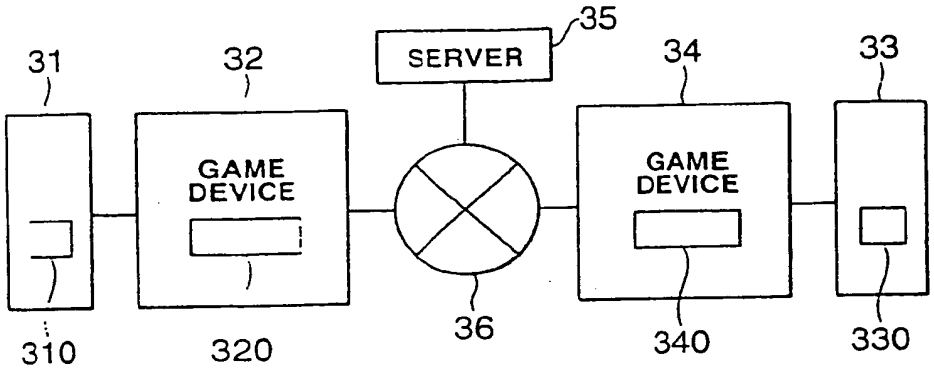

31
32
SERVER
35
34
33
GAME DEVICE
GAME DEVICE
36
310
320
340
330

FIG.5

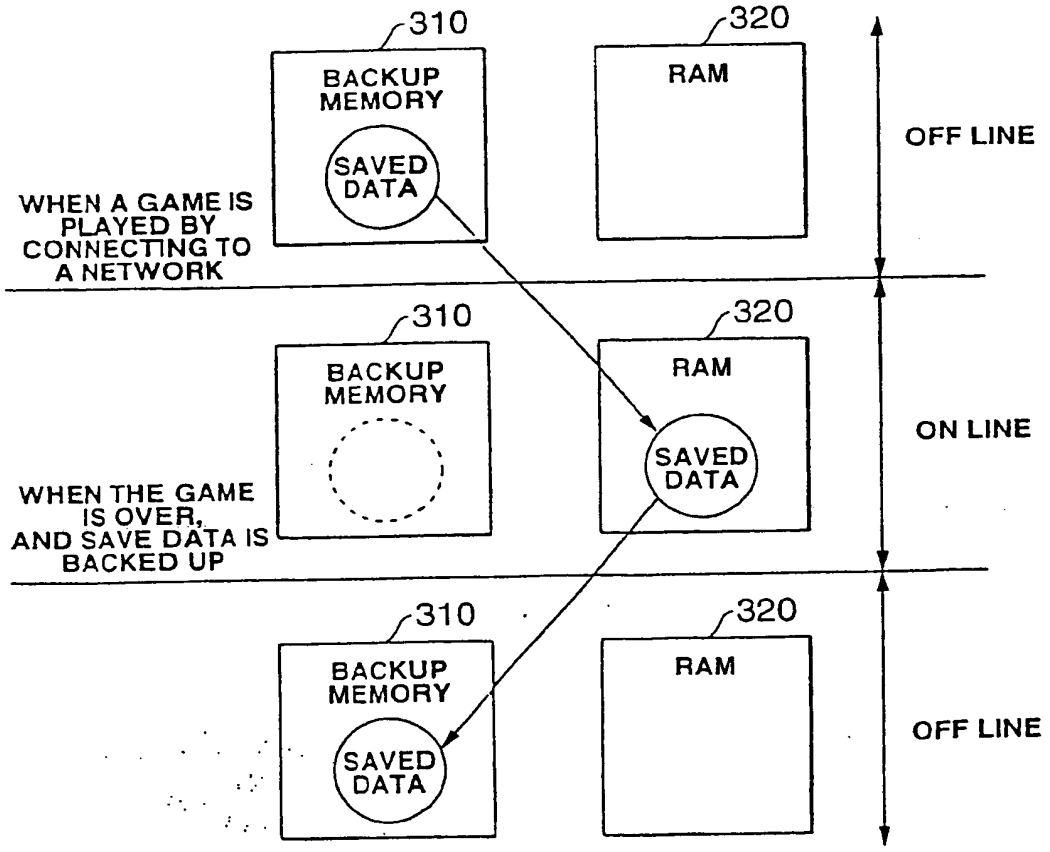

310
320
BACKUP MEMORY
RAM
SAVED DATA
OFF LINE
WHEN A GAME IS PLAYED BY CONNECTING TO A NETWORK
ON LINE
WHEN THE GAME IS OVER, AND SAVE DATA IS BACKED UP

FIG.6

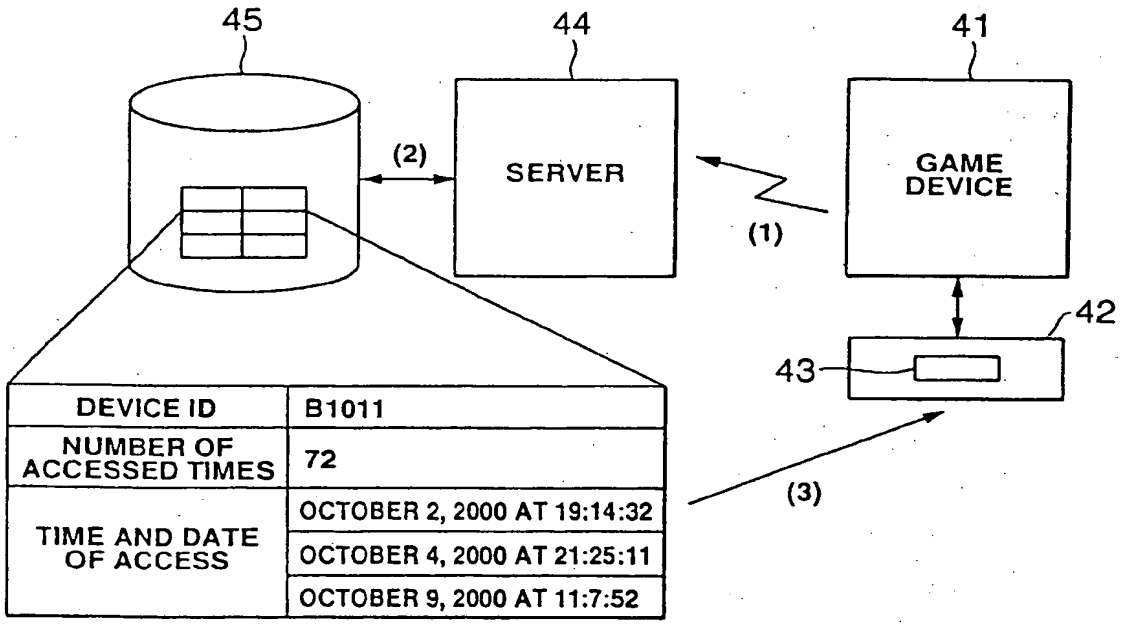

45
44
41
(2)
SERVER
GAME DEVICE
(1)
42
43
(3)
DEVICE ID
B1011
NUMBER OF ACCESSED TIMES
72
TIME AND DATE OF ACCESS
OCTOBER 2, 2000 AT 19:14:32
OCTOBER 4, 2000 AT 21:25:11
OCTOBER 9, 2000 AT 11:7:52

FIG.7

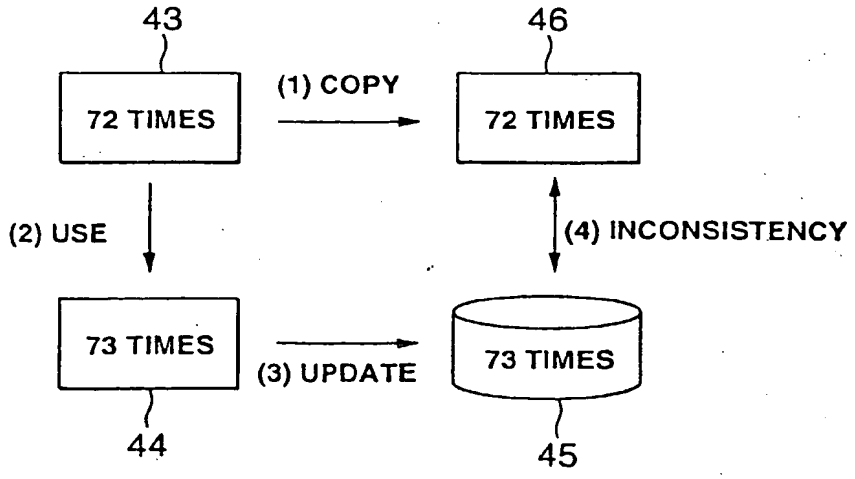

43
46
72 TIMES
(1) COPY
72 TIMES
(2) USE
(4) INCONSISTENCY
73 TIMES
(3) UPDATE
73 TIMES
44
45

FIG.8

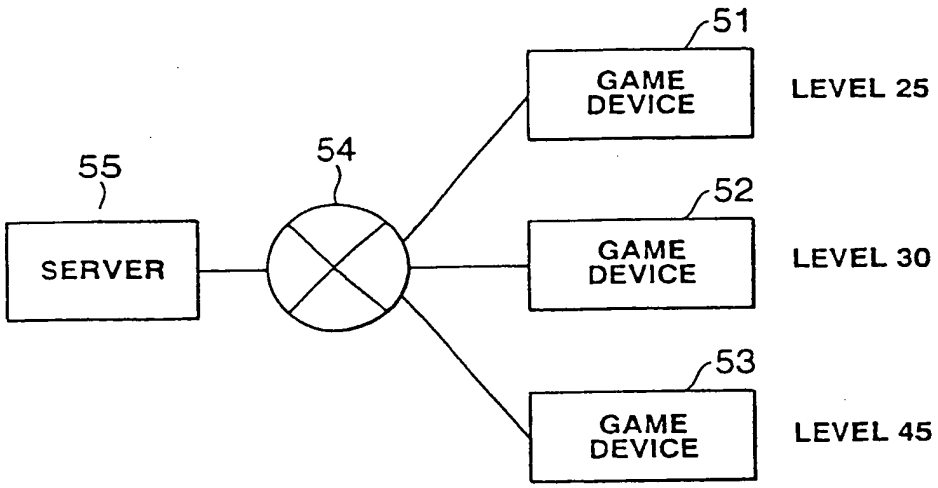


FIG.9

MODE	REQUIRED LEVEL
BASIC	NONE
ADVANCED	NO LESS THAN 20
EXPERT	NO LESS THAN 40

FIG.10

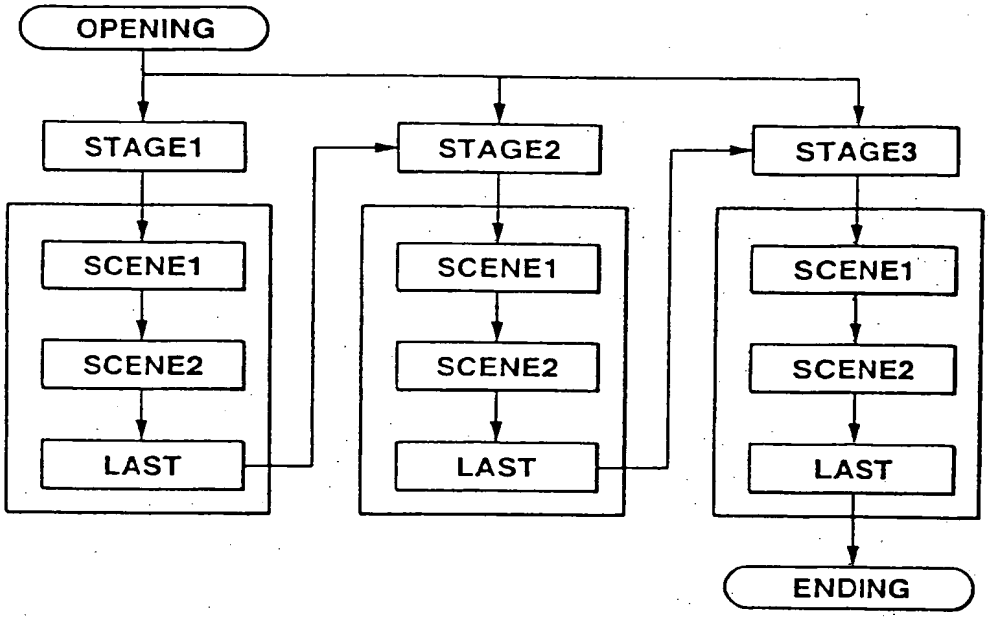
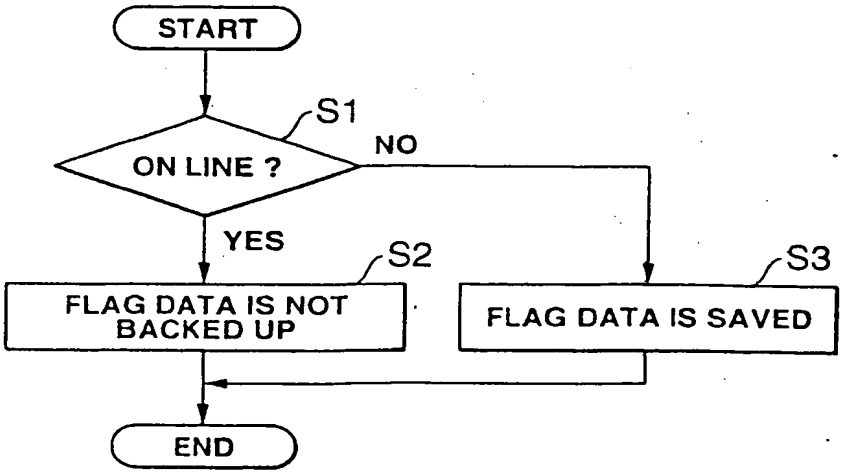


FIG.11



OFF LINE

FIG.12A

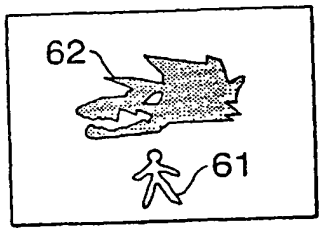


FIG.12B

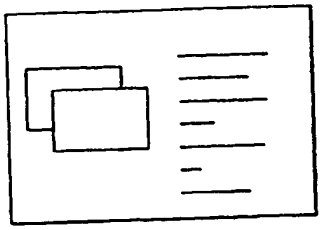
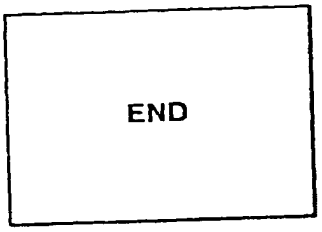


FIG.12C



ON LINE

FIG.12D

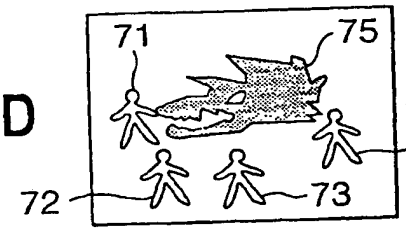
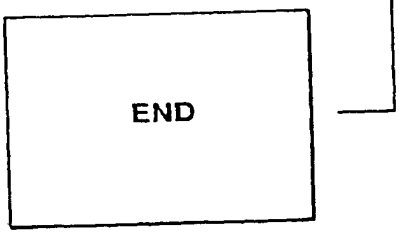


FIG.12E



(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 217 497 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
24.03.2004 Bulletin 2004/13

(43) Date of publication A2:
26.06.2002 Bulletin 2002/26

(21) Application number: **01310428.6**

(22) Date of filing: **13.12.2001**

(51) Int Cl.[7]: **G06F 1/00**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **20.12.2000 JP 2000387833**

(71) Applicant: **Sega Corporation**
Ohta-ku, Tokyo 144-8531 (JP)

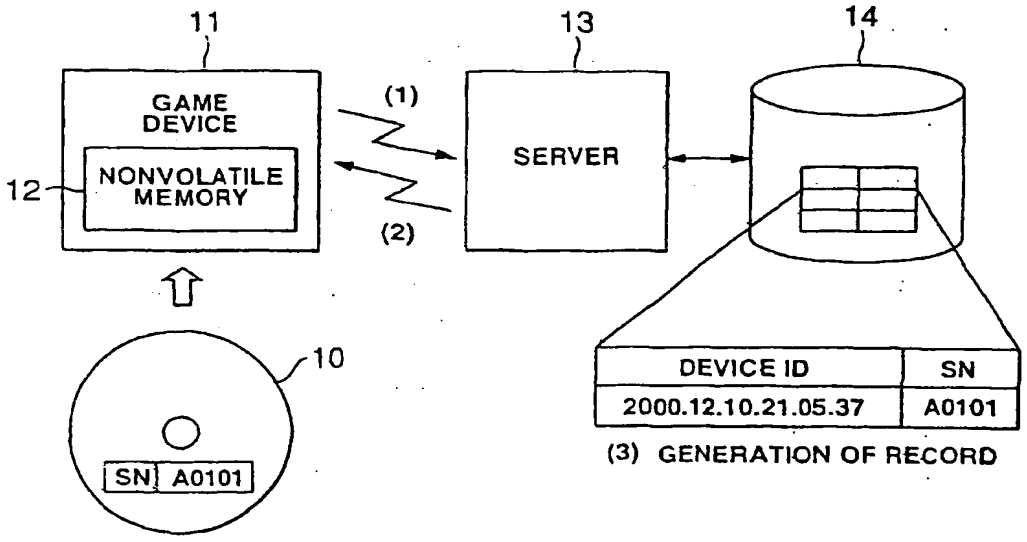
(72) Inventors:
- **Miyoshi, Takao**
  Ohta-ku, Tokyo 144-0043 (JP)
- **Setsumasa, Akio**
  Ohta-ku, Tokyo 144-0043 (JP)

(74) Representative: **Brown, Kenneth Richard**
R.G.C. Jenkins & Co.
26 Caxton Street
London SW1H 0RJ (GB)

(54) Security system for game devices connected with a server

(57) Provided is a security system for managing which CD-ROM is used for a game device not having identifying information in advance. When a game device accesses a server via a communication network, a device ID, which is issued from the server, is stored in a nonvolatile memory. This device ID is generated based on the time and date when the game device accesses the server via a communication network (e.g. December 10, 2000 at 21:05:37). The server associates a serial number (SN) of a CD-ROM used in the game device and a device ID of the game device with each other and registers them on a database .This makes it possible to manage which CD-ROM is used in each game device .

FIG.1



EP 1 217 497 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 31 0428

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 00/72119 A (RABIN MICHAEL O ;SHASHA DENNIS E (US)) 30 November 2000 (2000-11-30) * abstract * * page 5, line 11 - line 16 * * page 7, line 21 - page 10, line 9 * * claim 36 *	1-7	G06F1/00
X	US 5 790 664 A (COLEY CHRISTOPHER D ET AL) 4 August 1998 (1998-08-04) * column 14, line 12 - column 15, line 4 * * column 23, line 7 - line 24 *	1-7	
X	PATENT ABSTRACTS OF JAPAN vol. 2000, no. 05, 14 September 2000 (2000-09-14) -& JP 2000 035885 A (SEGA ENTERP LTD), 2 February 2000 (2000-02-02) * abstract *	1-7	
X	WO 00/58859 A (MICROSOFT CORP) 5 October 2000 (2000-10-05) * page 37, line 28 - page 38, line 12 * * claim 5 *	1-7	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F

~~The present search report has been drawn up for all claims~~

Place of search	Date of completion of the search	Examiner
Munich	11 November 2003	Anticoli, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

European Patent Office

Application Number
EP 01 31 0428

CLAIMS INCURRING FEES

The present European patent application comprised at the time of filing more than ten claims.

☐ Only part of the claims have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims and for those claims for which claims fees have been paid, namely claim(s):

☐ No claims fees have been paid within the prescribed time limit. The present European search report has been drawn up for the first ten claims.

LACK OF UNITY OF INVENTION

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

see sheet B

☐ All further search fees have been paid within the fixed time limit. The present European search report has been drawn up for all claims.

☐ As all searchable claims could be searched without effort justifying an additional fee, the Search Division did not invite payment of any additional fee.

☐ Only part of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the inventions in respect of which search fees have been paid, namely claims:

☒ None of the further search fees have been paid within the fixed time limit. The present European search report has been drawn up for those parts of the European patent application which relate to the invention first mentioned in the claims, namely claims:

1-7

European Patent Office

LACK OF UNITY OF INVENTION
SHEET B

Application Number
EP 01 31 0428

The Search Division considers that the present European patent application does not comply with the requirements of unity of invention and relates to several inventions or groups of inventions, namely:

1. claims: 1-7

   Independent claims 1, 3, 5-7 are directed towards managing which recording medium is used in each data processing evice

   ---

2. claims: 8-12

   Independent claims 8, 10 and 12 are directed towards managing saved data using backup means and encryption

   ---

3. claims: 13, 14

   Independent claims 13 and 14 are directed towards restoring saved data using backup means and deleting saved data backed up in the backup memory

   ---

4. claims: 15-19

   Independent claims 15, 17 and 19 are directed towards managing saved data in backup means using a progression number to check whether the backed up data is outdated after having been copied

   ---

5. claim: 20

   Independent claim 20 is directed towards managing difficulty levels in a communication game

   ---

6. claims: 21, 22

   Independent claims 21 and 22 are directed towards managing progression status's in a communication game

   ---

7. claims: 23, 24

   Independent claims 23 and 24 are directed towards reducing unnecessary online time in a communication game

   ---

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 31 0428

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

11-11-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0072119 A	30-11-2000	AU 767286 B2	06-11-2003
		AU 4813700 A	12-12-2000
		CA 2368861 A1	30-11-2000
		CN 1361882 T	31-07-2002
		EP 1180252 A2	20-02-2002
		JP 2003500722 T	07-01-2003
		WO 0072119 A2	30-11-2000
US 5790664 A	04-08-1998	AU 2054597 A	10-09-1997
		WO 9730575 A2	28-08-1997
JP 2000035885 A	02-02-2000	EP 1016960 A1	05-07-2000
		WO 9959058 A1	18-11-1999
		TW 393331 B	11-06-2000
		US 2003093639 A1	15-05-2003
		US 6510502 B1	21-01-2003
WO 0058859 A	05-10-2000	AU 3007800 A	16-10-2000
		AU 3380900 A	16-10-2000
		AU 3381000 A	16-10-2000
		AU 3503900 A	16-10-2000
		AU 3608100 A	16-10-2000
		AU 3708700 A	16-10-2000
		AU 3710100 A	16-10-2000
		EP 1287636 A2	05-03-2003
		EP 1259863 A2	27-11-2002
		JP 2003522989 T	29-07-2003
		JP 2003536119 T	02-12-2003
		WO 0057684 A2	05-10-2000
		WO 0059150 A2	05-10-2000
		WO 0059151 A2	05-10-2000
		WO 0058859 A2	05-10-2000
		WO 0058810 A2	05-10-2000
		WO 0059152 A2	05-10-2000
		WO 0058811 A2	05-10-2000
		US 2003078853 A1	24-04-2003
		US 2002012432 A1	31-01-2002
		US 2002007456 A1	17-01-2002
		US 2002013772 A1	31-01-2002

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82